

一年骗走美国人100多亿美元,老年人是受害人数最多的群体

印度的“电诈帝国”揭秘

“女士,您的逮捕令就在我的办公桌上,如果这个问题得不到解决,我们将不得不冻结您的账户,并将你关进监狱。我必须严肃地警告您,不要尝试与美国国税局抗争”。

这样一通号称来自“美国最强执法部门”——国税局的电话,会让大多数美国人陷入焦虑和恐慌,但电话另一头,“国税局工作人员”不经意间透露出的印度口音,预示着这可能是一场针对美国人的电信诈骗。

作为以英语为官方语言之一的人口大国,劳动力价格低廉的印度几乎承接了所有主要英语国家的电话呼叫业务,雇佣超过120万人。凭借这一产业的特殊资源,还滋生了一个庞大的“电诈帝国”,专门针对英语国家里最有钱的群体——美国公民。

据美国联邦调查局统计,2022年美国公民因网络电信诈骗损失了超过100亿美元(约合714亿元人民币),同比增长近4成,这些诈骗主要来自印度的呼叫中心。其中,老年人是受害人数最多的群体,光是他们就被骗走了超过30亿美元。

而近5年来,美国公民因网络电信诈骗造成的损失,已经超过了276亿美元。

精准诈骗

75岁的弗吉尼亚州退伍老兵布鲁恩,在5个月内被骗了近80万美元。

并不擅长使用电脑的布鲁恩,在网上遇到了一名冒充微软员工的骗子。骗子声称,布鲁恩的电脑遭到黑客攻击,他的财务账户遭到泄露,需要采取紧急补救措施。

在5个月的时间里,布鲁恩在骗子的指示下将毕生积蓄和退休金提取出来,转入一个加密货币账户。因为骗子告诉他,这个账户不会受到所谓的黑客攻击。

更糟的是,在布鲁恩的钱几乎被骗光后,真正的美国国税局通知他,因为提前提取了所有养老金,布鲁恩欠下了大约20万美元的税款。

目前,美国税法还没有为布鲁恩这样,因骗局而提取退休金的个人提供例外。

按照美国联邦调查局和美国司法部对电诈的分类,布鲁恩遇到的属于技术支持诈骗,主要针对老年人。利用美国人对印度人普遍擅长技术的刻板印象,这些身在印度的诈骗犯们,冒充美国知名科技公司的技术人员。



印度拥有全球规模最大的英语呼叫中心。



位于印度德里附近的古尔冈,一座灯火通明的呼叫中心。



印度街头的招聘广告,写着“急招电话员”。

近年来的电诈案件愈发普遍,以至于在美国政府部门的推动下,印度还专门设立了一个部门来处理呼叫中心针对美国人的电诈。

2020年8月,印度警方突击搜查了德里郊区古尔冈的一个呼叫中心,逮捕了20余名涉嫌诈骗美国公民的印度人。这些人在网上发布虚假的客服电话,并向受害者勒索高达700美元的“电脑维修费用”。

这个诈骗团伙的头目是一名身在迪拜的印度人,他每月付给这些员工400美元—500美元的薪水,待实施诈骗后再与美国当地称作“钱骡”的人群合作提现。

警方称,诈骗者接受过美国口音的训练,并被要求按照精心编排的剧本实施诈骗。他们通常

会冒充美国社会保障管理局、联邦调查局、国税局、国土安全部或缉毒局特工,威胁受害者如果不汇款,就会将他们逮捕、驱逐出境、吊销营业执照或驾驶执照。

针对老年人,印度骗子们也擅长通过彩票中奖、约会“杀猪盘”来进行诈骗。针对年轻人,印度骗子们还可以实施投资、贷款诈骗。而新移民们最怕的,无非就是犯罪和驱逐出境。

骗子们不但在人工话术上做到了真假难辨,在技术上甚至可以做到来电显示与美国官方部门热线电话一致。

“诈骗帝国”

印度在本世纪初期成为全球呼叫中心之都,跨国企业看中

印度庞大的英语人口基数和低廉的劳动力价格,纷纷将电话客服和销售外包给印度人。

当时,在印度的呼叫中心上班就是一份饱受误解但是收入令人羡慕的工作。

在论坛Quora的“在印度呼叫中心工作是什么体验”话题下,一名曾在呼叫中心工作过的员工表示,“我的房东曾经认为我是某种罪犯,因为我每天昼伏夜出,却过得很阔气。实际情况是,我的收入的确是当地平均水平的几倍,但时差让我只能上夜班。我还曾因身份不明被抓进警局,因为我们在工作中使用假名,在向美国人推销商品时,我有时是杰克,有时是詹姆斯。”

通过客户的个人信息去沟通,借用假名和假身份推销,早期印度呼叫中心的工作流程,与如今电诈的犯罪流程有着不少共同点。

印度呼叫中心的繁荣持续了大约10年,随着人力成本的上升,这些业务开始转移到劳动力价格更低的菲律宾等周边国家。

但有些从业者并不甘心让产业就这么衰落下去,这批有技术有能力的人们,从手头掌握的大量隐私信息上发现了可乘之机。

他们从有业务往来的科技公司手中窃取了客户的数据库,并且开始实施诈骗。很快,他们就发现电诈的成本有多低,回报有多丰厚。

据《今日印度》报道,在暗网上,只需花费5000卢比(约合428元人民币)即可访问高达100万人的个人数据。此类数据包括姓名、手机号码、地址、银行卡详细信息等。

常年在一线反诈的视频博主布朗宁(化名)在视频网站上有接近500万粉丝,本职为软件工程师的布朗宁表示,全球95%以上的诈骗电话都来自印度。根据布朗宁多年收集骗子的IP地址数据库来看,这些地址主要来自加尔各答、新德里及其周边地区。

相比于缅北,印度的诈骗产业规模更大,因为它面向的是十几亿英语人口和近10亿印地语人口。

而且印度的诈骗产业似乎很少传出“骗子们使用暴力胁迫普通人参与诈骗”的传闻,更多人是自愿从事诈骗的,他们认为发达国家的那些受害者有钱,并不在乎那些损失。

《纽约时报》曾通过布朗宁的技术手段,在线下约见了一名

印度的电诈骗子沙赫巴兹,却发现对方只是一个身材矮小、骨瘦如柴的年轻人,在面对采访时显得胆怯又寡言,和威胁受害者时咄咄逼人的形象大相径庭。

随着谈话的深入,沙赫巴兹一度似乎感到痛苦和愧疚。但在和记者分别不久后,沙赫巴兹又开始尝试诈骗另一名美国人。

打击困境

十年前,落后的印度贾坎德邦詹塔拉地区一度被称为“印度网络钓鱼之都”。

2020年有一部以当地故事为素材的网剧《詹塔拉:骗你没商量》上线,引起大量印度观众的共鸣。但如今,印度电诈窝点早已不止存在于那一片地区。

在印度北部的哈里亚纳邦、拉贾斯坦邦和北方邦,电诈产业“蓬勃发展”。随着经济复苏放缓,印度底层年轻人难以找到心仪的工作,工资高出当地平均收入水平四五倍的电诈产业,自然吸引不少人的加入。

一些不愿花成本培训员工的电诈组织,甚至还把目光瞄向了印度本国。从印度国会议员、宝莱坞演员,到一般的劳苦大众,都深受其害。

而印度警方对电诈的打击力度还远远不够。

根据印度警察研究与发展局的数据,电诈猖獗的拉贾斯坦邦仅在2023年4月,就收到超过来自当地人的10万起网络犯罪投诉,而该邦却只有两个专门应对网络犯罪的网络警察局。在超过14亿人口的印度,仅有29225名警察有资格调查网络犯罪案件。

连本国公民都顾不过来,印度警方几乎无暇顾及涉及外国人的诈骗案件。

警察管不过来,法律上的惩罚力度也不太够。在现行法律上,根据印度《信息技术法》,盗窃数据、密码、身份、发送网络钓鱼邮件或篡改计算机,仅可判处三年监禁。而且《信息技术法》中针对网络犯罪的大多数刑罚条款都是可以交钱保释的,对电诈罪犯的威慑力微乎其微。

对此,印度巴特那高等法院2022年才提出建议,表示需要打击网络犯罪分子的非法财富,并建议将他们的资产和金融交易置于所得税部门和执法局的审视之下。

另一方面,提高印度底层民众的反诈意识,并进行技术科普,则是一个更加漫长的过程。
据《时代周报》